Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] submits these comments in response to the Federal Communications Commission's ("Commission's") Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 ("*Further Notice*") proposing new requirements to address foreign-originated illegal robocalls.[2]

I. INTRODUCTION AND SUMMARY

USTelecom and its members appreciate the Commission's continued efforts to realize call authentication and to stop illegal robocalls. USTelecom agrees with the Commission that more action is necessary to address foreign-originated robocalls.[3] USTelecom also generally

[1] USTelecom is the premier trade association representing service providers and suppliers for the communications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its diverse membership ranges from international publicly traded corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country. USTelecom leads the Industry Traceback Group ("ITG"), a collaborative effort of companies across the wireline, wireless, VoIP and cable industries actively working to trace and identify the source of illegal robocalls. The ITG was first designated by the Commission as the official U.S. robocall traceback consortium in July 2020.

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105 (rel. Oct. 1, 2021) ("*Further Notice*").

[3] *See id.* ¶ 24 (tentatively concluding that the Commission's current rules are not sufficient to resolve the problem of foreign-originated illegal robocalls).

supports the Commission's focus on call transit, as it is critical to ensure that all calls destined to U.S. subscribers flow through a chain of trust from the originating provider to the terminating provider.

While further Commission action is necessary, the Commission should focus on new measures that will effectively and efficiently enhance the Commission's existing Robocall Mitigation Database ("RMD") approach and empower the Commission and industry to police providers. In particular, the Commission should streamline and enhance its approach to the RMD by closing the intermediate provider loophole and requiring that all providers, regardless of their role in the call path and whether or not they have implemented STIR/SHAKEN, implement a robocall mitigation program. In particular, as part of their robocall mitigation programs, intermediate providers should be expected to accept traffic only from other providers in the RMD. Enhancing the Commission's existing RMD approach – combined with active auditing of deficient database entries and aggressive and rapid enforcement – will help to foment trusted full call paths without causing unnecessary confusion and leaving opportunities for gamesmanship as a focus just on gateway providers would. The Commission also should ensure that any action taken pursuant to the *Further Notice* will indeed advance anti-robocalling efforts and not simply impose burdens on the voice service providers already leading the fight against illegal robocalls.

II. THE COMMISSION SHOULD STREAMLINE AND ENHANCE ITS EXISTING RMD APPROACH

Rather than adopting new conditional requirements that apply to providers when they play one role but not another, the Commission should work to streamline and enhance its existing approach. Specifically, the Commission should close the intermediate provider loophole and require all providers to have robocall mitigation programs, regardless of their

STIR/SHAKEN implementation status. Ensuring a full chain of trust in all calls destined to the U.S. with U.S. numbers is the better way to address foreign-originated robocalls.

A. The Commission Should Close the Intermediate Provider Loophole

USTelecom has previously advocated for the Commission to require intermediate providers to certify that they have implemented a robocall mitigation program, namely by committing to only directly accept calls from and to a U.S. number from providers in the RMD.[4] Imposing the certification obligation directly on all intermediate providers will better ensure that there is a chain of trust from the originating provider to the terminating provider, as intermediate providers would only take traffic from other intermediate providers that have also made the certification.

This approach will eliminate the loophole in the Commission's RMD regime that allows a provider to accept traffic from an upstream provider that is not in the database as long as that upstream provider did not originate the calls. The loophole currently breaks the "chain of trust" between the origination point of the call and the termination point, inviting service providers that are not known to the Commission and not committed to stopping illegal robocalls to routinely send traffic to U.S. consumers. Establishing a clear chain of trust that includes all intermediate providers will thus protect U.S. consumers and provide the Commission with a crucial tool to remove any problematic carrier from the call path by removing them from the RMD. It also will

[4] *See* Notice of Ex Parte Presentation of USTelecom, WC Docket No. 17-97, at 4 (filed Sept. 18, 2020) ("USTelecom Sept. 18, 2020 Ex Parte") ("[I]t is critical that intermediate providers also certify that they have implemented a robocall mitigation program, namely by committing to only directly accept calls from and to a U.S. number from U.S. providers in the Commission's Robocall Mitigation Database. Imposing this obligation directly on intermediate providers ensures that there is a chain of trust from the originating provider to the terminating provider, as intermediate providers would only take traffic from other intermediate providers that have made the certification.").

prevent providers from finding ways to "get in" the RMD to encourage others to accept their traffic, but without ever submitting a robocall mitigation plan or certifying to one.

In addition, requiring intermediate providers to be in the RMD will simplify compliance, including for the foreign providers trying to understand the commitments they are making by registering in the RMD. Under this approach, any provider that originates or transits calls using U.S. NANP resources destined to U.S. subscribers must be in the database and make a direct certification to the Commission. And all such providers must accept traffic only from other providers in the database, and must stand ready to cooperate in good faith in any tracebacks. This streamlined approach also will enhance industry and Commission policing of the call paths for illegal robocalls and work to complement traceback efforts.[5]

Closing the intermediate provider loophole also is sound public policy because it avoids discriminating against downstream service providers that establish direct relationships with originating service providers. Under the Commission's current approach, direct interconnection relationships are discouraged because the framework exempts traffic indirectly routed via intermediate providers from any registration requirement.

B. All Providers Should Be Required to Implement a Robocall Mitigation Program

As part of the certification in the RMD, the Commission should require that all providers implement a robocall mitigation plan, and that they do so regardless of the role in the call path they play and their STIR/SHAKEN implementation status. Specifically, the Commission should require all providers – whether serving as the gateway provider or otherwise – to certify that they have implemented an appropriate robocall mitigation program. For providers in their role as

[5] For instance, any time a traceback identifies a provider that is not in the RMD, downstream providers could be alerted of that fact as well as the Commission. Thus, each provider in the call path can more easily be held accountable, regardless of whether they are near the origination point or not.

immediate provider, an appropriate robocall mitigation plan would at minimum include their certification that they only accept traffic from other providers in the RMD, and that they will participate in good faith in tracebacks. The plan also should cover the process and actions that a provider takes to mitigate problematic traffic, whether received by a foreign or domestic entity, when the provider becomes aware of it, including when alerted of such traffic by the Commission or the traceback consortium.

In addition, providers' robocall mitigation programs should reflect at least a basic level of vetting of the providers from whom they directly accept traffic – beyond ensuring that they are registered in the RMD.[6] Accepting traffic from well-known providers (including well-known foreign providers regulated in their home countries) may not trigger the same concerns as accepting significant traffic from smaller, less known providers at home and abroad, given that small bad actors have a history of evading attempts to shut them down by simply establishing a new corporate entity and resuming business under another name.

While U.S.-based service providers were largely able to implement the Commission's RMD registration requirement with regard to foreign voice service providers that originate traffic, successful implementation of new rules that create a full chain of trust – which will include multiple foreign intermediate providers as well as foreign originating providers – will require more direct Commission involvement and interaction with foreign service providers.

[6] There is no way for intermediate providers to know the caller, or even the originating provider, in many if not most cases. In the context of intermediate providers, USTelecom recommends that the Commission avoid using the Know Your Customer terminology in the first instance, as it likely will create confusion regarding whether it applies to knowing the caller. *See Further Notice* ¶¶ 84-85 (seeking comment on Know Your Customer obligations and whether the upstream provider or call originator should be considered a gateway provider's "customer"). In addition, U.S. service providers cannot reasonably be expected to police the activities or registration status of any service provider (whether domestic or foreign) with which they do not have a direct relationship.

These efforts also will take time.[7] Many international intermediate providers have no direct relationship with U.S. providers and may not be informed of U.S. laws and regulations. Thus, the Commission should undertake awareness-building with foreign service providers and foreign regulators, including by issuing clear public guidance to help foreign service providers readily understand the registration process and what certification requires of them.

As part of a new certification requirement, the Commission should not require new filings of providers that already have submitted robocall mitigation program. Rather, the Commission should require those providers to update their plans as necessary. It also should require that providers indicate in the RMD the role or roles they play in the ecosystem, including as an originating provider and/or as an intermediate provider, and whether they directly accept traffic from foreign providers.[8] This could be done as easily as adding checkboxes to the RMD where providers could indicate whether they act as originating providers, intermediate providers, and/or foreign providers. Finally, the Commission should remove from the RMD any provider currently in the database that was imported as an intermediate provider.

The robocall mitigation program requirement should apply to all providers, regardless of their STIR/SHAKEN implementation status. One consequence of STIR/SHAKEN implementation is that bad actors may increasingly make illegal robocalls with their own numbers, and there is already evidence of some bad actors doing so.[9] STIR/SHAKEN provides

[7] The rules should not take effect internationally until the Commission has confirmed foreign providers are aware of the new rules, and capable of and intent on stepping into this new regime.

[8] As part of updates to the RMD regime, the Commission should require that providers that update their filings input additional information that will help other providers identify them through the RMD, such as Operating Company Numbers (OCNs) and Access Customer Name Abbreviations (ACNAs).

[9] *See* Comments of USTelecom – The Broadband Association, WC Docket No. 13-97, WC Docket No. 07-243, WC Docket No. 20-67, IB Docket No. 16-155, at 2, 5-6 (filed Oct. 14, 2021).

important information about whether the calling number can be trusted, but it does not indicate whether a given call is legal or illegal, good or bad.[10] In contrast, a robocall mitigation program obligates providers to do more to prevent their networks from being used to originate illegal robocalls, and allows the Commission to hold them accountable when they fail to do so.

C. The *Further Notice's* Specific Focus on Gateway Providers May Create More Confusion and Loopholes to the Existing Regime

The Commission should work to improve and enhance the existing regime in the ways suggested above, rather than adopt new requirements that apply to providers when they play certain roles but not others. Indeed, gateway provider-specific rules may be counterproductive.

A straightforward consistent approach, in contrast to a new set of sometimes applicable rules, aids compliance and accountability. As USTelecom recently noted in comments in the Commission's direct access to numbering resources proceeding, the Commission's robocall regime already includes myriad rules that apply and sometimes overlap, creating a complex framework to navigate but without necessarily covering all scenarios where providers contribute to illegal robocalls.[11] The Commission should not add additional complexity with rules that apply when providers act as gateway providers but not when they play other roles.

Indeed, rules that apply to providers only when they act as gateway providers, but not in other contexts, threatens to add new opportunities for gamesmanship. For instance, some providers may claim to be based in the United States – and even may be legal U.S. corporate entities – but have little or no U.S. presence, operations, or principals. The threat of enforcement may not have a significant deterrence effect against such entities. In addition, some gateway providers may be fly-by-night entities that, in effect, rely on another provider's (including

[10] *Id.* at 2.

[11] *See id.* at 3-6.

potentially downstream transit provider's) platform to accept and route calls. These providers very well could disappear upon any significant scrutiny, only for one or more gateway providers to pop up in place. These facts obfuscate which provider – whether the gateway provider or the provider one or two hops downstream – is most responsible and can best be held accountable by the Commission for bringing foreign-originated illegal traffic to U.S. subscribers. In some cases, this obfuscation may very well be by design.

Rather than adopt new gateway-specific obligations, the Commission should focus on ensuring trust and accountability through the entire call path through the more straightforward approach described above. Should the Commission take that approach, it would be unnecessary to, for example, require that gateway providers block calls based on Commission notification of illegal calls,[12] as the Commission could rely on the RMD and its existing bad actor provider blocking safe harbor to achieve the same goal more broadly.[13]

D. The Commission Must Aggressively and Rapidly Enforce Its Regime

A key to unlocking the promise of the RMD of a chain of trust in all U.S.-destined traffic is aggressive and rapid enforcement. The Commission today already has a significant set of tools to ensure that providers are held accountable, which will be enhanced with the changes to the RMD proposed herein. The Commission can and should take action to ensure that RMD filings are proper and valid, and take action when they are not.

For instance, USTelecom has previously flagged that many providers have redacted their robocall mitigation plans in their entirety, often without following either Commission procedures

[12] *See Further Notice* ¶ 57.

[13] For these reasons, although USTelecom does not generally oppose a 24-hour traceback cooperation requirement, *see id.* ¶ 52, it may not make sense to impose such requirement specifically on gateway providers.

to request confidentiality or the Commission's Protective Order requirements.[14] In addition to undermining the purpose of the plans and the RMD, redacting robocall mitigation plans in their entirety would appear to amount to a false certification that "[t]he filer also certifies that the attached **searchable** PDF details the specific reasonable steps it has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, and, if applicable, the type of extension or extensions it received under 47 CFR § 64.6304."[15]

In addition, the Commission should – informed by industry traceback results – actively audit the database to ensure that foreign service providers that are indirectly sending traffic to the United States through intermediate foreign providers are adhering to their RMD commitments. It should then actively take appropriate action (including industry notification) to remove any registrant that does not comply with that registrant's certification. The need to ensure compliance with RMD obligations are administrative and investigative functions the Commission itself must perform.

III. ANY NEW REQUIREMENTS SHOULD MATERIALLY REDUCE ILLEGAL ROBOCALLS AND NOT IMPOSE UNJUSTIFIED BURDENS

A. A Requirement to Authenticate Unauthenticated Calls Would be Unduly Burdensome and Would Fail Any Reasonable Cost-Benefit Analysis

The Commission previously struck the right balance with regard to when intermediate providers must authenticate unauthenticated calls, requiring that such providers do so only if they do not cooperate with traceback.[16] The Commission should not depart from that balanced

[14] *See* Reply Comments of USTelecom – The Broadband Association, WC Docket No. 17-97, at 3 (filed June 8, 2021).

[15] *See* FCC, Robocall Mitigation Database, Certifications (emphasis added).

[16] *See Further Notice* ¶ 39; *see also* USTelecom Sept. 18, 2020 Ex Parte at 7-8.

approach, regardless of the fact that the choice between traceback cooperation and authentication was mooted by the agency's traceback mandate.[17]

Several USTelecom members serve as gateway providers for substantial amounts of traffic destined to the U.S., but despite that quantity, are virtually never identified as the Point of Entry for high-volume illegal robocalls. Instead, as indicated by the cases recently brought by the Commission and its federal and state counterparts, lesser known providers, including some small VoIP providers, most often serve as the gateways for illegal traffic.[18] The proposed requirement may have little or no impact on the actions of these providers, yet will require substantial costs of USTelecom members to upgrade their gateways that essentially bring only legal traffic into the United States.

Just as critically, the requirement also would serve almost no benefit in the effort to reduce and eliminate illegal robocalls. Although the STIR/SHAKEN call authentication framework is a critical component of restoring trust in the telephone network, the proposed requirement will not meaningfully advance it. In most scenarios where foreign-originated traffic

---

[17] *Id.* ¶ 40.

[18] *See, e.g.,* FCC, Press Release, FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams from United States Telephone Network (Apr. 3, 2020), https://docs.fcc.gov/public/attachments/DOC-363522A1.pdf (describing warnings to SIPJoin, Connexum, and VoIP Terminator/BLMarketing); FCC, Press Release, FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Covid-19-Related International Scammers (May 20, 2020), https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf (describing warnings to RSCom and PTGi Carrier Services), FCC, Press Release, FCC Demands Two More Companies Immediately Stop Facilitating Illegal Robocall Campaigns (May 18, 2021), https://docs.fcc.gov/public/attachments/DOC-372543A1.pdf (describing warnings to VaultTel Solutions and Prestige DR VoIP); United States of America vs. Nicholas Palumbo, *et al*., Civil Action No. 20-CV-473, Complaint, para. 8, p.4 (E.D.N.Y) (Jan. 28, 2020); State of Vermont Attorney General's Office, Press Release, Attorney General Donovan Announces Settlement with Scam Robocall Carrier (Apr. 28, 2021), https://ago.vermont.gov/blog/2021/04/28/attorney-general-donovan-announces-settlement-with-scam-robocall-carrier/ (describing settlement with Strategic IT Partner); State of Indiana Office of Attorney General, Event Announcement (Oct. 14, 2021), https://events.in.gov/event/attorney_general_todd_rokita_files_lawsuit_against_alleged_robocalling_scammers?utm_campaign=widget&utm_medium=widget&utm_source=State+of+Indiana (announcing lawsuit against Startel Communications).

is not authenticated, gateway providers will only be able to assign a C-level attestation to such traffic.[19] C-level attestation was included in the standard primarily for the benefit of traceback, but the industry traceback process has advanced to become so quick and efficient that C-level attestations offer at best a marginal benefit for traceback.[20] Indeed, the industry traceback process today already successfully identifies the providers that bring substantial numbers of illegal robocalls into the United States. Nor will C-level attestations provide additional useful information for terminating providers' analytics, as terminating providers ultimately may treat C-level attestations from untrusted providers the similar to unauthenticated calls.[21]

In this regard, any marginal benefit that a gateway provider attestation requirement could bring in mitigating illegal robocalls would in no way cover the substantial costs – up to eight figures for some providers – to deploy the upgrades necessary to do so. The upgrade process is more than just expensive: Replacing and updating existing gateway infrastructure to add capabilities to sign traffic would involve multiple years of complex project management activity. The thousands of person-hours required for the effort would be far better deployed for other projects that could bring far more meaningful protections to consumers.

[19] *Cf. id.* ¶ 45 ("To the extend standards allow a gateway provider to assign "full" (A-level) or "partial" (B-level) attestation to a call, under this proposal they are free to do so; they would not be limited to assigning "gateway" (C-level) attestation."); *see also* Comments of Belgacom International Carrier Services SA, CG Docket No. 17-59, WC Docket No. 17-97, at 3 (filed Nov. 22, 2021). Notably, the SHAKEN standards consider cross-border traffic and international calls potentially can be signed by originating carriers abroad. *See* Comments of the Alliance for Telecommunications Industry Solutions, CG Docket No. 17-59, WC Docket No. 17-97, at 7 (filed Dec. 6, 2021).

[20] *See* Notice of Ex Parte Presentation of USTelecom, WC Docket No. 17-97, at 2 (filed Sept. 1, 2020).

[21] Worse, if any gateway providers inappropriately sign illegal robocalls with A-level attestations, it could cause direct harm to providers' reliance on STIR/SHAKEN information before that malfeasance is detected.

B. Call Blocking Mandates Are Unnecessary and May Cause Unintended Consequences

The Commission should not mandate that voice service providers block calls, regardless of their position in the call path and whether the calls are from invalid, unallocated, or unassigned numbers, or numbers on a do-not-originate ("DNO") list.[22] Importantly, blocking mandates can cause unintended consequences. Even invalid or unallocated numbers sometimes today are used for legitimate calls, inadvertently because of caller misconfigurations or in other narrow contexts. Mandated automatic blocking therefore can lead to the blocking of legitimate calls, including some critical ones. Moreover, because many terminating providers already undertake sophisticated blocking and labeling of calls they deem highly likely to be illegal and/or illegal or unwanted based on reasonable analytics, there would be limited benefit to gain of a blocking mandate further upstream.

There likewise is no reason for the Commission to require gateway or any other providers to block calls from numbers on a DNO list. The current permissive approach to DNO is robust and ensures that calls on industry DNO lists are highly unlikely to reach subscribers. Today, 40+ providers, including virtually every major transit and terminating provider, directly receive the DNO list the Industry Traceback Group ("ITG") maintains on behalf of the industry. Major analytics providers also receive the list. Given this broad distribution, numbers on the list almost certainly will be blocked somewhere along the call path before reaching subscribers. Indeed, some gateway providers receive the ITG's list, either directly or through an analytics provider or vendor. Those providers may block the calls at that point of the call path. Even if calls from DNO numbers get beyond the gateway, because every major transit provider receives the ITG's

[22] *See Further Notice* ¶ 67 (proposing to require gateway providers to use reasonable analytics to block calls highly likely to be illegal); *id.* ¶ 72 (proposing to require gateway providers to block calls on a DNO list).

list and most traffic runs through at least one of them, the calls likely will be blocked there. Large terminating providers also receive the ITG's list, meaning that, in the unlikely event the calls make it that far, the terminating providers will then block the calls. Extending the reach beyond ITG members, the analytics providers and vendors that receive the list may block or label the calls on behalf of the providers they work with or consumers they support, further reducing the likelihood that any calls from numbers on the list make it to subscribers.

There also are additional protections in the ecosystem that complement the ITG's DNO list. For instance, Somos and Neustar maintain their own DNO lists that they make available broadly across the industry. Callers also can register numbers that they do not use to originate calls with the major analytics providers to inform the analytics engines' blocking and labeling efforts. These measures allow additional numbers beyond those on the central ITG list to receive effective DNO treatment, without the same technology challenges that occur with network-based DNO blocking in legacy systems.[23]

The practical effect of the combination of these efforts is that calls today from numbers on DNO lists are highly unlikely to reach subscribers. They may be blocked by major transit or terminating providers, the analytics partners of terminating providers, or others – all before they cause the phone to ring. If any get through providers' network blocking, they may still be labeled as likely spam or fraudulent, thanks to additional protections in the ecosystem. Thus, there is no additional benefit of requiring gateway providers to block calls from numbers on the

[23] The ITG specifically requires that numbers are actively being spoofed and at high volume to be included in the list. This is because many providers, particularly those with legacy equipment, cannot add an indefinite amount of DNO numbers nor seamlessly update the list in all of their switches and equipment. This can include the switches and equipment they use for gateways. Accordingly, if the Commission's desire is to expand the extent of the numbers on a central DNO list, doing so would raise substantial practical and technical challenges.

same lists since the calls are highly unlikely to make it all the way to the subscriber in the first instance.

IV. CONCLUSION

USTelecom agrees with the Commission that more action is necessary to address foreign-originated illegal robocalls. Instead of adopting new requirements focused exclusively on gateway providers, the Commission instead should work to refine and enhance its existing RMD regime, including by ensuring that all providers in the call path have robocall mitigation programs and are in the RMD. Doing so will help to ensure a full chain of trust in the call path of calls destined to the U.S. subscribers – and will aid accountability when that chain is broken.

Respectfully submitted,

By: */s Joshua M. Bercu /*

Joshua M. Bercu
Vice President, Policy & Advocacy

USTelecom – The Broadband Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 551-0761

December 10, 2021